Method and device for high-security multifunction electronic control comprising a microchip card

Patent Number: FR2637710

Publication date: 1990-04-13

Inventor(s): BRECHET MICHEL

Applicant(s): B ET DEV (FR)

Requested Patent: ☐ FR2637710

Application Number: FR19880013393 19881007

Priority Number(s): FR19880013393 19881007

IPC Classification: G06F13/00; G06F15/21; G06K19/02

EC Classification: G06K19/073, G06K19/077, G07F7/10D8P, G07F7/10D10M

Equivalents:

Abstract

The subject of the present invention is a method and devices for high-security multifunction electronic control. They comprise a casing with a keyboard, a screen and a connector allowing dialogue with a microchip card which is inserted into the said casing. A microprocessor incorporated in the latter then allows configuration of the card which is in the form of a known credit card for chosen functions. It comprises, in particular, a zone 102 for intelligent connecting on hearing a card code emitted by the casing and then making the operation processing zone 101 active. A microprocessor 7, of low capacity, decodes the pulses transmitted and compares the result with a code recorded in the non-relative and partitioned memory 8. A second microprocessor 5, then accessible, is associated with a memory zone 6 divided into specialised memories for the chosen functions. 

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 637 710**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **88 13393**

(51) Int Cl⁵ : G 06 F 15/21, 13/00; G 06 K 19/02.

(12) DEMANDE DE BREVET D'INVENTION A1

(22) Date de dépôt : 7 octobre 1988.

(30) Priorité :

(43) Date de la mise à disposition du public de la demande : BOPI « Brevets » n° 15 du 13 avril 1990.

(60) Références à d'autres documents nationaux apparentés :

(71) Demandeur(s) : *Société anonyme dite : B + DEVELOPMENT.* — FR.

(72) Inventeur(s) : Michel Brechet.

(73) Titulaire(s) :

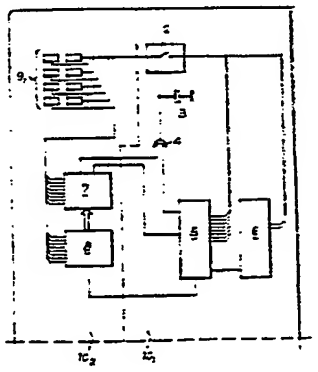
(74) Mandataire(s) : Cabinet Beau de Loménie.

(54) Procédé et dispositif de commande électronique multifonction à haute sécurité comportant une carte à puce.

(57) La présente invention a pour objet un procédé et des dispositifs de commande électronique multifonction à haute sécurité. Ceux-ci comprennent un boîtier avec un clavier, un écran et un connecteur permettant un dialogue avec une carte à puce que l'on insère dans ledit boîtier. Un microprocesseur incorporé dans celui-ci permet alors de configurer la carte qui se présente comme une carte de crédit connue pour des fonctions choisies.

Elle comporte, en particulier, une zone 10_2 de connectique intelligente à l'écoute d'un code carte émis par le boîtier et rendant alors active la zone 10_1 de traitement d'opérations. Un microprocesseur 7, de faible capacité, décode les impulsions transmises et compare le résultat avec un code enregistré dans la mémoire 8 non relative et fragmentale.

Un deuxième microprocesseur 5 alors accessible est associé à une zone mémoire 6 divisée en mémoires spécialisées pour les fonctions choisies.



FR 2 637 710 - A1

2637710

Procédé et dispositif de commande électronique multifonction à haute sécurité comportant une carte à puce.

DESCRIPTION

La présente invention a pour objet un procédé et des dispositifs de commande électronique multifonction à haute sécurité comportant une carte à puce.

Le secteur technique de l'invention est celui de la fabrication des cartes à mémoire ou à puce programmable, lassociée à un boîtier de contrôle et de configuration de cette carte.

Une des applications de l'invention est par exemple l'usage d'une même carte d'une part en monétique comme les cartes de crédit connues et d'autre part en clé d'accès, ouvrant droit à l'usage de matériels ou de locaux protégés avec différents niveaux de sécurité ou à des fichers d'informations privatifs ou collectifs.

On connaît déjà des dispositifs utilisant des cartes à mémoire ou à puce dans différentes fonctions de commandes électroniques et de transactions essentiellement en monétique. La plupart de ces cartes n'ont qu'une seule fonction, même quand elles sont associées à un boîtier de contrôle qui permet de dialoguer avec elles pour, par exemple, en changer un mode opératoire.

On peut citer par exemple dans la fonction monétique, qui est à ce jour la plus répandue, le brevet anglais déposé le 30 Janvier 1981 sous le No GB 81 02894 par Mr CHALMERS David, intitulé "Carte de crédit programmable" (Adaptable value token) qui reprend l'état de la technique au jour de son dépôt et qui revendique une carte monétique pouvant sélectionner différents modes opératoires à partir d'un clavier intégré à celle-ci avec un écran de visualisation, un code d'accès non modifiable et une interface avec des terminaux par piste magnétique.

Dans le même domaine, un autre brevet anglais, antérieur au précédent, a été déposé le 20 Décembre 1979 sous le NO 79 43832 par la Compagnie W. LETHABY and CO, intitulé "Dispositif d'opération financière" (Transaction device),et qui décrit du reste une partie de ce qui est repris dans le brevet précédent.

Dans le domaine des contrôles d'accès par identification, on peut citer le brevet US No 349862, déposé le 10 Avril 1973, sous priorité de trois brevets suisses, par Mr KURT EHRAT et intitulé "Système d'identification d'individus" (Identification system for individuals) qui décrit un dispositif comportant une station centrale et des unités d'identification portable; dans le même domaine, le brevet US, déposé le 31 Mars 1978 sous le No 7910799 par PITNEY BOWES INC. WALNUT and PACIFIC STREETS, et intitulé "Système d'accès à un ordinateur" (Computer accessing system) revendique un dispositif portable avec clavier et afficheur connectable à un ordinateur et permettant un accès codé à celui-ci.

Dans le domaine des dispositifs multifonctions, on relève le brevet US No 99797, déposé le 03 Décembre 1979 par la Société I.B.M. et intitulé "Système de sécurité pour la vérification de code d'accès" (A system for achieving secure password verification) qui décrit en fait une carte à mémoire connectable à un terminal à clavier avec des systèmes de sécurité qui permettent une identification réciproque comme dans les cartes de crédit connues et pouvant être utilisée dans d'autres domaines mais avec des cartes spécialisées pour chacun et éventuellement des boîtiers portables individuels assurant l'interface entre la carte et le terminal.

Enfin, on citera le brevet UK No 8002325, déposé le 23 Janvier 1980 par Douglas John PYNE et intitulé "Carte magnétique de poche et encodeur" (Portable pocket magnetic token and encoder) qui revendique une carte magnétique à mémoire comportant un clavier et afficheur pouvant être connectée à divers terminaux pour divers usages spécialisés en monétique ou en accès de locaux par exemple.

On note ainsi dans ces divers exemples que chaque système ou carte est finalement dédié à une seule fonction même si au départ il peut s'adapter à diverses utilisations. Son usage est défini initialement en fonction des terminaux d'ordinateurs où il sera connectable pour des opérations déterminées dans un domaine unique.

Par ailleurs, la sécurité est toujours basée sur un code d'accès porté par le système ou la carte et un autre éventuellement dans le terminal mais leur décodification peut être réalisée assez facilement indépendamment l'un de l'autre, ce qui constitue une

faiblesse que beaucoup de fabricants et surtout d'utilisateurs déplorent en subissant alors des violations d'accès très préjudiciables suivant le domaine concerné.

Enfin la plupart des dispositifs de commande électronique comportent des cartes qui sont soit à puce ou à mémoire passives et ne comportent que des mémoires de stockage d'informations entièrement accessibles même, si elles sont protégées par des codes et des circuits inhibiteurs, par un lecteur externe dans lequel on les introduit et qui est connecté lui-même par exemple à un ordinateur sur lequel l'opérateur peut éventuellement agir, soit à puces actives et comportant elles-mêmes un clavier et un écran de contrôle ne permettant plus donc de les utiliser sans risque de détérioration comme une carte de crédit dans un terminal de type bancaire connu. Chacune de ces configurations est limitée alors dans son utilisation.

Le problème posé est de pouvoir commander tout appareil nécessitant une protection d'accès par une commande électronique comportant une carte à puce de telle façon que le niveau de sécurité soit de très haute qualité et que l'on puisse utiliser la même carte pour plusieurs usages successifs et en particulier être compatible avec les terminaux monétiques connus.

Une solution au problème posé est un procédé de commande électronique multifonction utilisant une carte à puce comportant au moins un microprocesseur et un boîtier portable associé comportant au moins un clavier alphanumérique, un microprocesseur, un connecteur compatible avec ladite carte à mémoire et une source d'alimentation, caractérisé en ce que :

- on connecte la carte à puce au boîtier et on entre au clavier de ce boîtier un code confidentiel qu'on a préalablement choisi et stocké dans une zone mémoire non volatile de ladite carte ou dudit boîtier;

- on compare, par le microprocesseur de la carte et celui du boîtier, le code introduit au clavier avec celui préalablement stocké et s'ils sont identiques, on choisit, par le clavier, une fonction d'utilisation parmi plusieurs préalablement définies et stockées dans une mémoire de ladite carte;

- on configure cette carte pour la fonction choisie grâce aux microprocesseurs incorporés dans le boîtier et dans la carte;

- on retire la carte à mémoire du boîtier et on la présente à tout terminal fixe externe correspondant à ladite fonction d'utilisation;

- on utilise d'une manière connue ladite carte qui permet l'accès et l'usage dudit terminal pour la fonction choisie.

En option, on fixe à la construction dans une mémoire fixe et non programmable de la carte, un code imposé par l'organe gérant ledit terminal de la fonction choisie et on fait correspondre par une table d'équivalence incorporée à ladite carte un code personnel choisi par l'utilisateur de telle façon que ce code personnel est validé par ledit terminal et permet l'accès et l'usage de celui-ci.

Une autre solution au problème posé est un dispositif de commande électronique multifonction constitué d'une carte à puce et d'un boîtier associé comportant une source d'alimentation, un connecteur compatible avec ladite carte à puce et un clavier alphanumérique, caractérisé en ce que ladite carte comporte deux zones, l'une incluant une mémoire non volatile mais fragmentable, un microprocesseur de faible capacité spécialisé pour décoder les impulsions d'un code envoyé par le boîtier et les comparer à celui choisi et préalablement enregistré dans ladite mémoire non volatile, un système de commutation électronique commandé par ledit processeur et alimentant alors la deuxième zone de la carte qui inclue un microprocesseur principal et ses circuits accessoires connus programmés pour pouvoir sélectionner les fonctions d'utilisation à travers le clavier du boîtier et une zone à mémoire associée au microprocesseur principal et stockant toute information nécessaire aux fonctions d'utilisations possibles de la carte, lequel boîtier associé comporte un microprocesseur et ses circuits accessoires connus et une zone mémoire associée à ce microprocesseur dans laquelle sont stockées les informations fichier et les codes nécessaires au fonctionnement dudit boîtier et à la mise en service et en configuration pour une fonction déterminée de ladite carte à puce.

Le résultat est un nouveau procédé et dispositif de commande électronique utilisant une carte à puce et un boîtier associé.

Les avantages d'un tel procédé et dispositif sont multiples : en premier lieu, il permet un usage multifonction de la carte à puce, en particulier en fonction bancaire à la place de toute autre carte de crédit actuelle connue mais aussi en fonction accès à des locaux, et à certains fichiers de données privatifs ou collectifs ce qui réduit le nombre de cartes que doit porter une personne; en effet, les systèmes à carte se développent et chaque groupement, organisme, collectivité ou individu possède une carte propre à la fonction qui le concerne, obligeant alors toute personne affiliée ou membre doit posséder autant de cartes que d'accès auxquels alors il a droit, augmentant les risques de perte, d'oubli et de violation de ses droits; la présente invention permet à l'utilisateur de n'avoir qu'une seule carte pour toutes ces fonctions.

En deuxième lieu, le procédé et le dispositif selon l'invention apporte un niveau de sécurité de très haute qualité vis à vis de tentative d'utilisation frauduleuse du système et des cartes à mémoire en particulier. En effet, la présence de microprocesseurs dans le boîtier et dans la carte, associés à des mémoires mortes et vives et leur programmation par dialogue réciproque obligatoire sont déjà un premier niveau de sécurité puisque dans les systèmes actuels l'ensemble de la programmation est en général porté par un seul support alors que dans la présente invention, il est séparé sur deux supports.

Ainsi le procédé et le dispositif selon l'invention garantissent d'une part l'inviolabilité de l'emploi de l'une des deux parties séparément et d'autre part des deux parties ensemble sans connaissance du code d'utilisation commun.

De plus, on peut rajouter des codes de sécurité à différents niveaux, lesquels codes étant, soit fixés au départ et inaccessibles par la suite par l'utilisateur mais accesibles par l'organisme gérant la fonction associée au travers de ses terminaux et lui permettant ainsi d'identifier le porteur de la carte et d'autoriser l'accès à ladite fonction, soit reprogrammables par l'utilisateur lui-même ou par l'organisme gérant une fonction donnée, certains de ces codes persistant même en cas d'absence de source d'alimentation.

Un avantage pratique réside dans l'utilisation du code personnel choisi par l'utilisateur pour toute validation exigée dans

certaines transactions sur des terminaux (monétiques en particulier) et non du code imposé à priori par l'organisme gérant la fonction, le plus souvent difficile à mémoriser par l'utilisateur.

Un autre avantage du procédé et du dispositif selon l'invention est que les cartes à mémoire ne seront pas détériorées par les terminaux, ce qui est souvent le cas des cartes qui comportent par exemple leur clavier incorporé. Ainsi le coût d'exploitation est diminué et la carte elle-même est d'un prix de revient limité, alors que le boîtier, s'il est plus onéreux, est réutilisable indéfiniment et même si les cartes ont elles une durée de vie limitée fixée par l'organisme gérant une des fonctions de la carte. Une autre économie indirecte est réalisée également en utilisant un seul boîtier pour plusieurs cartes.

La description suivante se réfère au schémas et aux dessins annexés qui représentent, sans caractère limitatif, un exemple de réalisation du procédé et du dispositif suivant l'invention et qui est donné à titre d'illustration mais d'autres réalisations peuvent être envisagées.

- La figure 1a est une vue en perspective de dessus d'un dispositif suivant l'invention.

- La figure 1b est une vue en perspective de dessous d'un dispositif suivant l'invention.

- La figure 2 est un schéma des connections internes de la carte à puce entre ses différents composants.

- La figure 3 est un schéma de connection du boîtier.

La figure 1a représente le dispositif suivant l'invention en vue perspective de dessus et comprenant un boîtier 13 portable, de petite dimension, dans lequel est glissée une carte à puce 1 par exemple de format et de nature connue comme les cartes de crédit, ledit boîtier formant alors un étui de protection de celle-ci.

Le boîtier 13 comporte un clavier alphanumérique 11, un écran éventuel de contrôle 14, piloté par un microprocesseur interne au boîtier tel que décrit dans la figure 3 et une découpe 16 à l'une de ses extrémités pour pouvoir saisir la carte et la sortir du boîtier grâce également à l'ouverture décrite dans la figure 1b.

Pour réduire la taille du boîtier qui peut être d'une dimension à peine supérieure à celle de la carte pour faciliter son usage, le clavier est extra-plat et l'écran peut être à cristaux liquides.

La figure 1b représente le dispositif suivant l'invention en vue perspective de dessous. On retrouve la carte 1 glissée dans le boîtier 13 et pouvant être retirée facilement grâce à une ouverture 15 pratiquée dans le fond du boîtier, à la découpe 16 décrite dans la figure 1a et à la flexibilité de la carte à mémoire 1. Les formes de l'ouverture 15 ou de la découpe 16 peuvent être quelconques.

Le boîtier comporte, pour être portable, outre ses circuits internes décrits dans la figure 3, un logement pour des piles interchangeables 12 fournissant l'énergie nécessaire.

Il peut comporter également, à partir de ce logement ou extérieurement, une prise de connection pour une alimentation extérieure permettant en particulier de fournir un voltage spécial suivant le type de composants nécessaires aux mémoires choisies du circuit interne en fonction des utilisations de la carte.

La connection entre la carte 1 et le boîtier 13 est réalisée par un organe de communication 9 qui, dans un mode de réalisation préférentiel est un connecteur électrique normalisé de type octopolaire tel que Bull CP8 installé dans les normes de géométrie convenable mais qui peut être aussi par exemple une liaison optique ou à induction par bobines.

On peut envisager également de rajouter sur le boîtier dans les circuits décrits dans la figure 3 différentes fonctions tel que le réveil avec une sonnerie et tout type d'affichage à l'écran de différentes informations stockées dans une mémoire comme dans tout appareil portable électronique connu tels qu'une montre, une calculatrice, des agendas, etc. Le boîtier peut ainsi servir à stocker des données permanentes.

On peut également, en option, rajouter une piste magnétique externe pour la rendre compatible avec un lecteur correspondant.

La figure 2 est un schéma des connections internes de la carte à puce 1 qui peut être en particulier physiquement conforme aux normes de la carte bancaire comme présentée dans la figure 1. Elle comporte de surcroît une couche matérielle logicielle qui permet d'assurer diverses fonctions telles que l'accès aux terminaux

bancaires, l'accès à des locaux protégés ou à tout système de stockage confidentiel de données privatives ou collectives. Cette couche matérielle et logicielle est schématisée sur cette figure 2 et n'est alimentée électriquement en énergie et en ordre actif qu'à travers l'organe de communication 9_1 relié au boîtier décrit dans la figure 3 quant la carte est insérée dans ledit boîtier.

La carte 1 comprend en fait deux zones : une zone 10_2 que l'on peut appeler de connectique intelligente capable d'être à l'écoute d'un code carte reçu et de rendre active la zone 10_1 et donc toute la carte si et seulement si le code correct est reçu à travers l'organe de liaison 9_1 et une zone 10_1 de traitement d'opérations bancaires et autres, rendue passive tant que la zone 10_2 n'a pas reçu le code d'activation correct.

Ledit organe de communication 9_1 ou plus simplement le connecteur dans un mode particulier de réalisation, est relié à un microprocesseur 7 de faible capacité et spécialisé. Il décode les impulsions transmises par le connecteur et compare le résultat avec un code préalablement enregistré dans une zone mémoire 8. Celle-ci est une mémoire non volatile mais fragmentable, type EEPROM ("Electrical Erasable Programmable Read Only Memory") c'est-à-dire fixe même sans alimentation et programmable, qui comprend au moins une capacité de deux octets; celle-ci permet d'une part de stocker un code confidentiel initial qui devra correspondre après à celui reçu par le connecteur 9_1 mais qui peut être ensuite modifié, et d'autre part éventuellement de compter le nombre de mauvaises introductions du code reçu.

En effet, si celui introduit par exemple dans le clavier du boîtier 13, et celui préalablement stocké dans la mémoire 8 ne sont pas identiques, on peut n'autoriser qu'un nombre limité d'essais répétitifs d'un autre code introduit au clavier et quand ce nombre est atteint on rend par exemples les autres fonctions de la zone 10_1 de la carte inaccessible. Ce capteur peut être remis à zéro à chaque reconnaissance du code valide.

Le connecteur 9_1 est également relié à un système de commutation électronique 2 permettant, sous contrôle d'une fonction logique 4 de type "ou", la connection ou la déconnection du connecteur 9_1 avec la zone 10_1. La fonction logique 4 est commandée

soit par un signal élaboré par le microprocesseur 7 au début des opérations lorsque le code d'activation est connu, soit par un signal issu d'un autre microprocesseur 5 pour maintenir la connection pendant un travail de la zone 10_1 sur une opération correspondant à une fonction choisie et pour une durée également choisie quand la carte est ensuite sortie du boîtier.

Un élément de temporisation 3, qui peut être un simple condensateur, permet en effet le maintien de l'activation de la carte pendant une durée déterminée qui peut être par exemple d'une minute.

Le système de commutation 2 permet l'alimentation et la commande d'un microprocesseur principal et de ses circuits accessoires connus, tels que horloge, décodeur, multiplexeurs, latch etc. ... regroupés dans l'ensemble 5. Celui-ci n'est actif que s'il reçoit de l'énergie du connecteur 9_1 et une fois activé, il contrôle l'état du microprocesseur 7 en lui imposant par exemple l'arrêt de la recherche d'un éventuel code envoyé à travers le connecteur 9_1 . Il peut remettre également à zéro le compteur d'erreurs de la mémoire 8.

Enfin le système de commutation 2 permet également l'alimentation de la zone mémoire 6 associée au microprocesseur 5; celle-ci comprend autant de parties spécialisées que de fonctions souhaitées, en particulier elle peut comporter :

- une partie figée fixe et non programmable ("ROM" ou " Read Only Memory") qui est typiquement pour une application bancaire pour recueillir le code imposé et les informations données par l'organisme concerné;

- une partie programmable fixe et non volatile ("Electrical Erasable Programmable Read Only Memory EEPROM") pour les applications vie privée;

- une partie volatile pour permettre des calculs et l'accès à des fichiers intermédiaires pendant le temps de connection à un terminal de service pour la fonction choisie ou au boîtier 13.

On notera que chaque liaison représentée sur le schéma peut être un nombre de liaisons électriques physiques pour aller de 1 à plus de 16, et qu'il s'agit d'un exemple de réalisation possible mais non limitative de connections internes.

En particulier, dans un mode de réalisation préférentiel, ladite carte à puce 1 comporte en outre une table d'équivalence qui

fait correspondre un code choisi par l'utilisateur, modifiable par lui et confidentiel, que l'on peut qualifier de personnel, et préalablement stocké dans une des mémoires de la carte (qui peut être, pour simplifier, le même que celui stocké dans la mémoire 8 de la zone 10_2 et nécessaire pour ouvrir le commutateur 2) à celui imposé par l'organisme de gestion de la fonction choisie et figé définitivement dans la mémoire fixe et non programmable de la zone 10_1. Ainsi, lors de l'utilisation de ladite carte 1, configurée préalablement par le boîtier pour son usage dans un terminal de la fonction choisie, on utilise le code personnel ci-dessus en lieu et place du code initial imposé par l'organisme gérant. Ladite table d'équivalence permet alors une validation de la correspondance entre le code personnel envoyé par le clavier du terminal au travers du système de commutation 2 et le code imposé ,et autorise ainsi l'accès à la fonction dudit terminal.

La figure 3 est un schéma interne de connexion du boîtier 13 qui peut être physiquement de la forme externe tel que décrit dans la figure 1. Les circuits internes de ce boîtier comportent une alimentation en énergie électrique 12 par piles interchangeables ou par prise de connection interne, laquelle alimentation fournit à chaque composant dudit boîtier la puissance électrique nécessaire par les bornes 17_1 et 17_2 correspondantes.

Dans un mode de réalisation préférentiel, un des composants principaux est un microprocesseur 18 avec ses circuits connus accessoires de contrôle et de division de signaux, non représentés ici par souci de simplification,
tels que : horloge, multiplexeurs, latch et sérialisateurs de données, lequel microprocesseur a une zone mémoire 21 associée dans laquelle sont stockés les informations fichées et les codes nécessaires au fonctionnement dudit boîtier et à la mise en service et en configuration pour une fonction déterminée de ladite carte à puce.

Le microprocesseur 18 peut piloter un écran de contrôle 14 qui peut être à cristaux liquides et qui est entièrement sous contrôle de ce microprocesseur. Les ordres donnés à celui-ci par l'utilisateur sont transmis par la frappe des touches d'un clavier 11 de type connu.

Un système de détection 19 de la carte décrit dans la figure 2 permet de vérifier la présence de celle-ci en bonne place comme par exemple grâce à des contacts à encliquetage activés quand la carte est en butée dans la configuration tel que décrit dans les figures 1.

Un système d'interrupteur électronique 20 permet alors l'envoi sur les bornes de l'organe de communication 9_2 avec la carte à puce, les tensions d'alimentation, la réception et l'émission de données à destination et en provenance du microprocesseur 18 et tous les signaux de contrôle nécessaires à la connectique de l'organe de communication qui peut être un connecteur électrique normalisé connu de type octopolaire tel que Bull CP8.

Ainsi l'interrupteur électrique 20 est normalement dans un état de coupure, découplant les bornes du connecteur de tout signal électrique. L'introduction de la carte à puce en bonne place dans le boîtier active l'interrupteur et le connecteur.

On notera que chaque liaison représentée sur le schéma peut être un nombre de liaisons électriques physiques pour aller de 1 à plus de 8 et qu'il s'agit d'un exemple de réalisation possible mais non limitative des connections internes.

Ledit boîtier 13, que l'on peut appeler transacteur, permet donc, par les composants ci-dessus et un dialogue
avec ceux de la carte, d'activer ladite carte à puce 1, grâce à la programmation des droits d'accès commandant les serrures électroniques décrites. Le transacteur peut permettre ainsi d'identifier la carte elle-même, d'inscrire sur la carte dans un fichier réservé, un code d'accès correspondant à une porte ou à une famille de portes, de générer un code secret à l'usage du détendeur de la carte à mémoire pour permettre un accès sécurité renforcé, à enregistrer au profit d'un réseau informatique, la nature et la date de cette ouverture de droits.

Certains de ces codes sont modifiables à volonté par l'usager et peuvent être dotés d'une durée de vie programmée, ce qui permet une délégation temporaire des droits.D'autres restent toujours en vigueur par la carte elle-même comme pour les utilisations bancaires ou ne peuvent être lus et/ou modifiés par l' organisme gérant une fonction donnée.

Dans un mode de réalisation particulier, on peut fixer à la construction dans les mémoires respectives de ladite carte et dudit boîtier un code unique confidentiel auquel l'utilisateur n'a plus accès par la suite afin de rendre les deux parties indissociables.

Ledit boîtier 13 peut servir également, grâce à une zone mémoire convenable, de stockage temporaire de l'ensemble des informations stockées préalablement sur la carte à puce 1 et que l'on veut retranscrire sur une nouvelle carte, le délai de péremption de la première étant écoulé. Il suffit dans ce cas de transférer les informations à transcrire de la carte initiale vers le boîtier qui sert alors de relais puis du boîtier vers la nouvelle carte.

La présente invention n'est pas limitée aux modes de réalisations décrits ci-dessus et qui ne constituent que des exemples auxquels des variantes et des modifications peuvent être apportées.

REVENDICATIONS

1. Procédé de commande électronique multifonction utilisant une carte à à puce (1) comportant au moins un microprocesseur (7) et un boîtier portable (13) associé comportant au moins un clavier alphanumérique (11), un microprocesseur(18), un connecteur (9) compatible avec ladite carte à puce et une source d'alimentation(12), caractérisé en ce que :

- on connecte la carte à puce (1) au boîtier (13) et on entre au clavier (11) de ce boîtier un code confidentiel qu'on a préalablement choisi et stocké dans une zone mémoire non volatile de ladite carte ou dudit boîtier;

- on compare, par le microprocesseur (7) de la carte et celui (18) du boîtier, le code introduit au clavier avec celui préalablement stocké et s'ils sont identiques, on choisit, par le clavier, une fonction d'utilisation parmi plusieurs préalablement définies et stockées dans une mémoire de ladite carte (1).

- on configure cette carte pour la fonction choisie grâce aux microprocesseurs incorporés dans le boîtier et dans la carte;

- on retire la carte à puce du boîtier (13) et on la présente à tout terminal fixe externe correspondant à ladite fonction d'utilisation;

- on utilise d'une manière connue ladite carte qui permet l'accès et l'usage dudit terminal pour la fonction choisie.

2.Procédé de commande électronique suivant la revendication 1, caractérisé en ce que si le code introduit au clavier (11) et celui préalablement stocké ne sont pas identiques, on autorise un nombre limité d'essais répétitifs d'un autre code introduit au clavier et quand ce nombre est atteint, on rend les fonctions de la carte définitivement inaccessibles.

3. Procédé de commande électronique suivant la revendication 1 ou la revendication 2, caractérisé en ce que l'on fixe à la construction, dans les mémoires respectives de ladite carte et dudit boîtier, un autre code unique confidentiel auquel l'utilisateur n'a plus accès par la suite afin de rendre les deux parties indissociables.

4. Procédé de commande électronique suivant l'une quelconque des revendications 1 à 3, caractérisé en ce que l'on fixe à la

construction dans une mémoire fixe et non programmable de ladite carte (1), un code imposé par l'organisme gérant le terminal d'une fonction choisie, et on fait correspondre, par une table d'équivalence incorporée dans ladite carte, un code personnel choisi par l'utilisateur de telle façon que ce code personnel est validé par ledit terminal et permet l'accès et l'usage de celui-ci.

5. Dispositif de commande électronique multifonction constitué d'une carte à puce (1) et d'un boîtier associé (13) comportant une source d'alimentation (12) , un connecteur (9) compatible avec ladite carte à puce et un clavier alphanumérique (11) caractérisé en ce que ladite carte comporte deux zones, l'une (10_2) incluant une mémoire (8) non volatile mais fragmentable, un microprocesseur (7) de faible capacité spécialisé pour décoder les impulsions d'un code envoyé par le boîtier et les comparer à celui préalablement enregistré dans ladite mémoire non volatile, un système de commutation électronique (2) commandé par ledit processeur et alimentant alors la deuxième zone (10_1) de la carte qui inclue un microprocesseur (5) principal et ses circuits accessoires connu programmés pour pouvoir sélectionner les fonctions d'utilisation à travers le clavier du boîtier et une zone mémoire (6) associée au microprocesseur principal et stockant toute information nécessaire aux fonctions d'utilisations possibles de la carte, lequel boîtier (13) associé comporte un microprocesseur (18) et ses circuits accessoires connus et une zone mémoire (21) associée à ce microprocesseur dans laquelle sont stockées les informations-fichier et les codes nécessaires au fonctionnement dudit boîtier et à la mise en service et en configuration pour une fonction déterminée de ladite à carte à puce.

6. Dispositif de commande électronique selon la revendication 5, caractérisé en ce que la zone mémoire (6) associée au microprocesseur principal de ladite carte (1) comporte au moins une partie figée fixe et non programmable.

7. Dispositif de commande électronique suivant la revendication 5 ou la revendication 6, caractérisé en ce
que la zone mémoire (6) associée au microprocesseur principal de ladite carte (1) comporte au moins une partie programmable fixe et non volatile.

8. Dispositif de commande électronique suivant l'une quelconque des revendications 5 à 7, caractérisé en ce que la zone mémoire (6) associée au microprocesseur principal de ladite carte (1) comporte au moins une partie volatile.

9. Dispositif de commande électronique suivant l'une quelconque des revendications 5 à 8, caractérisé en ce que ledit boîtier (13) comporte un écran de contrôle (14) entièrement sous contrôle du microprocesseur (18).

10. Dispositif de commande électronique suivant l'une quelconque des revendications 5 à 9, caractérisé en ce que ladite carte à puce (1) comporte un élément de temporisation (3) permettant le maintien de l'activation de la carte pendant une durée déterminée.

11. Dispositif de commande électronique suivant l'une quelconque des revendications 5 à 10, caractérisé en ce que la carte à puce (1) et le boîtier (13) sont reliés par un connecteur électrique (9) normalisé de type octopolaire.

12. Dispositif de commande électronique suivant l'une quelconque des revendications 6 à 11, caractérisé en ce que la carte à puce (1) respecte les normes de toute carte bancaire connue, de type carte de crédit et est utilisable en fonction monétique par l'introduction d'un code propre à cette fonction, reconnu par les terminaux bancaires, stocké dans la partie de sa mémoire figée, fixe et non programmable et activable seulement par le boîtier.

13. Dispositif de commande électronique suivant l'une quelconque des revendications 5 à 11, caractérisé en ce que le boîtier (13) est également un étui de protection de ladite carte à puce (1).

14. Dispositif de commande électronique suivant l'une quelconque des revendications 5 à 13, caractérisé en ce que ledit boîtier (13) comporte une zone à mémoire dans laquelle l'ensemble des informations préalablement stockées sur la carte à puce (1) peut être transféré, puis de laquelle lesdites informations sont transcrites sur une nouvelle carte.

15. Dispositif de commande électronique suivant l'une quelconque des revendications 5 à 14, caractérisé en ce que ladite carte (1) comporte une table d'équivalence qui fait correspondre un code personnel choisi par l'utilisateur à celui imposé par l'organe

de gestion d'une fonction choisie, laquelle table d'équivalence permet une validation entre lesdits codes par le clavier du terminal dudit organisme et autorise l'accès à la fonction choisie.

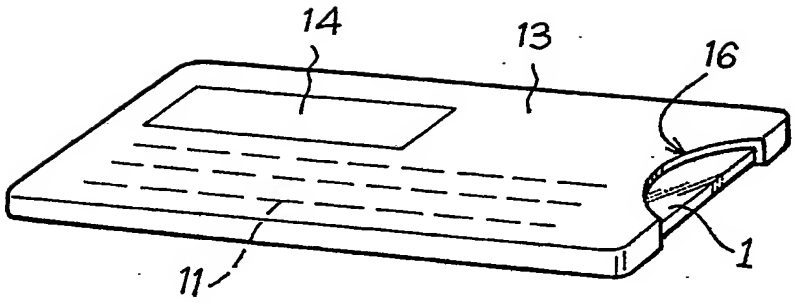


Fig_1a

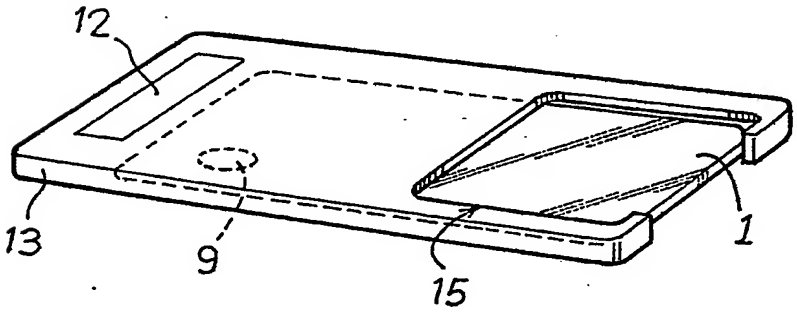


Fig_1b

213

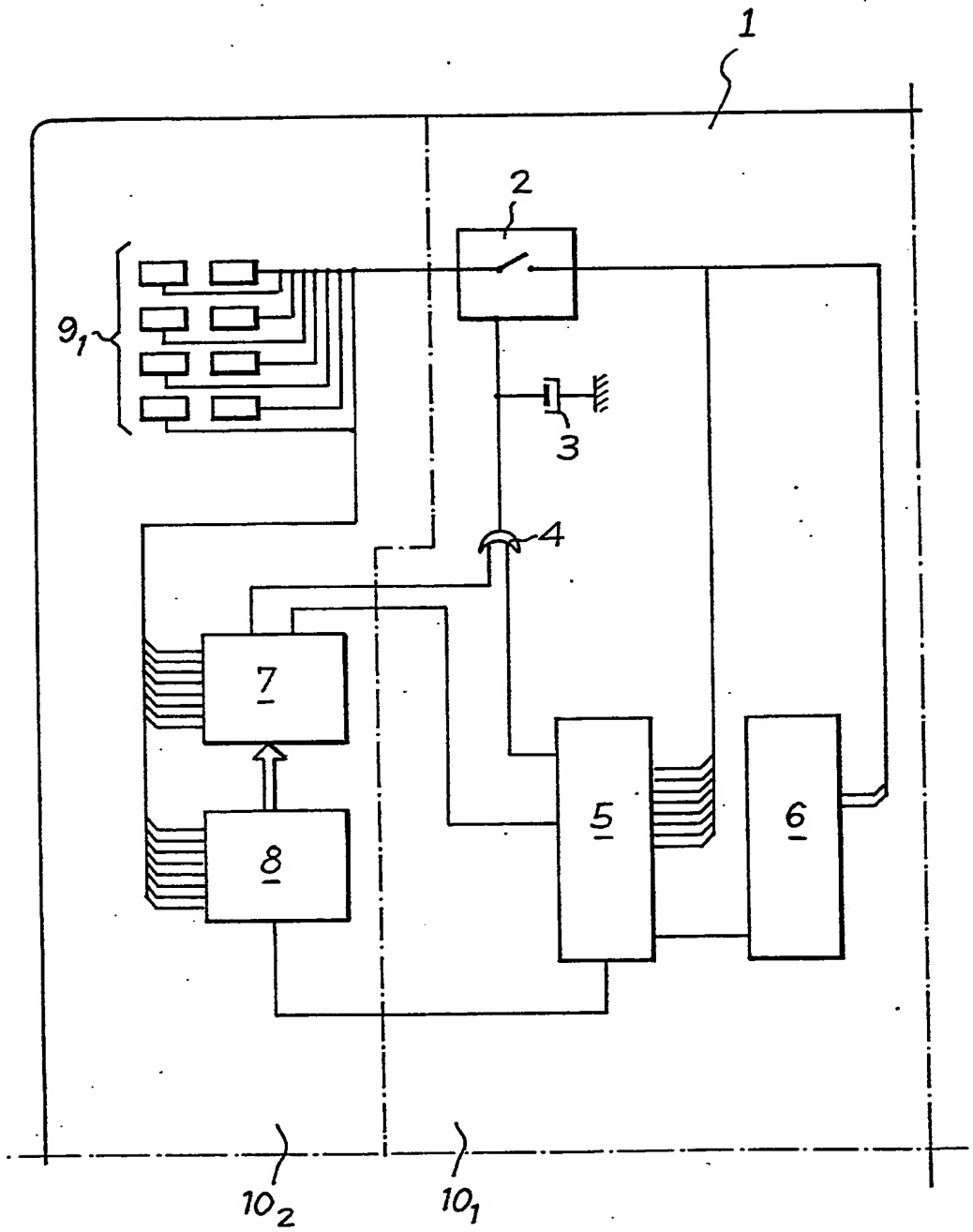


Fig-2

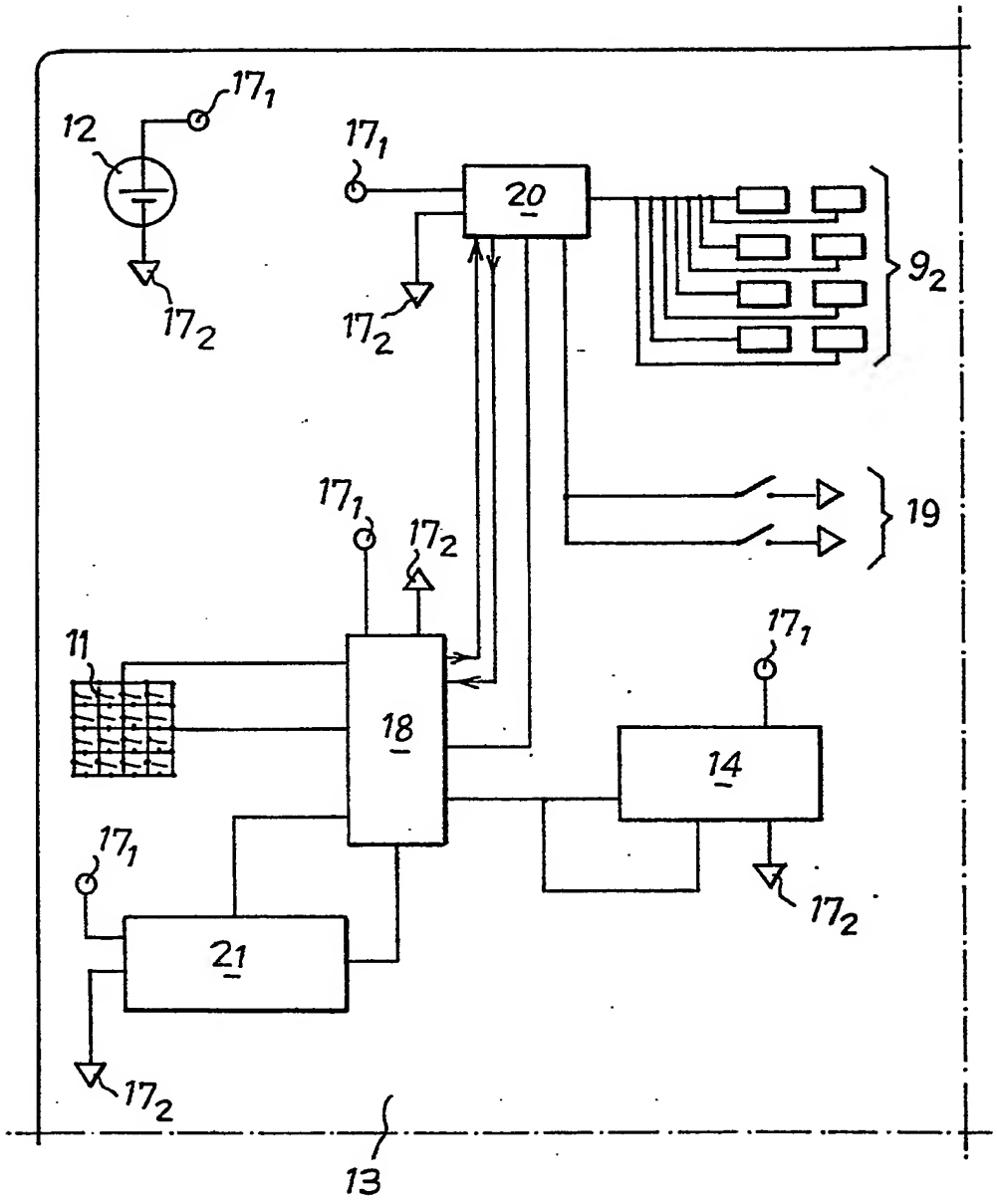


Fig-3